



الحمد لله عالم السر والنجوى ، والصلاة والسلام علي من لا ينطق عن الهوى ، وعلي اله وصحبه ومن لزم الرشاد والهدى ، اما بعد

2

دورة أمن الهواتف الذكية

اساسيات الحماية في نظام ios

قناة لرفع الملفات المرئية والنصية
الصادرة عن مؤسسة آفاق الإلكترونية
Telegram.me/Horizons_lib
مكتبة آفاق

دورة امن الهواتف الذكية

الدرس الثاني

اساسيات الحماية في نظام

IOS



نظام IOS

نظام تشغيل مغلق المصدر مطور من شركة أبل ، حسب تسريبات إدوارد سنودن الأخيرة فإن وكالة الامن القومي الامريكي كانت تتجسس علي سيرفرات شركة أبل وتزامن بيانات المستخدمين من خلال برنامج Prism ، مازالت شركة أبل تتعاون مع أجهزة الاستخبارات الأمريكية بدعوي الأمن القومي الأمريكي ومكافحة الإرهاب ففي عملية سان برنانديو بولاية كالفورنيا ساعدت شركة أبل مكتب التحقيقات الفيدرالي الأمريكي FBI بمشاركة جميع البيانات الموجودة علي سيرفرات أبل لمنفذ العملية لكنها رفضت انشاء باب خلفي في نظام التشغيل بشكل كامل لانه سيؤثر سلبا علي جميع مستخدمي أيفون

لذا هذه أساسيات الحماية بنظام iOS للحد من مشاركة بياناتك ومعلوماتك مع شركة أبل لا سيما خدمة التخزين السحابي iCloud

هذه الخطوات ستمنحك مساحة للتنفس للحفاظ علي خصوصيتك ولكنها لن تعزلك بشكل كامل عن شركة أبل

- تحديث النظام -

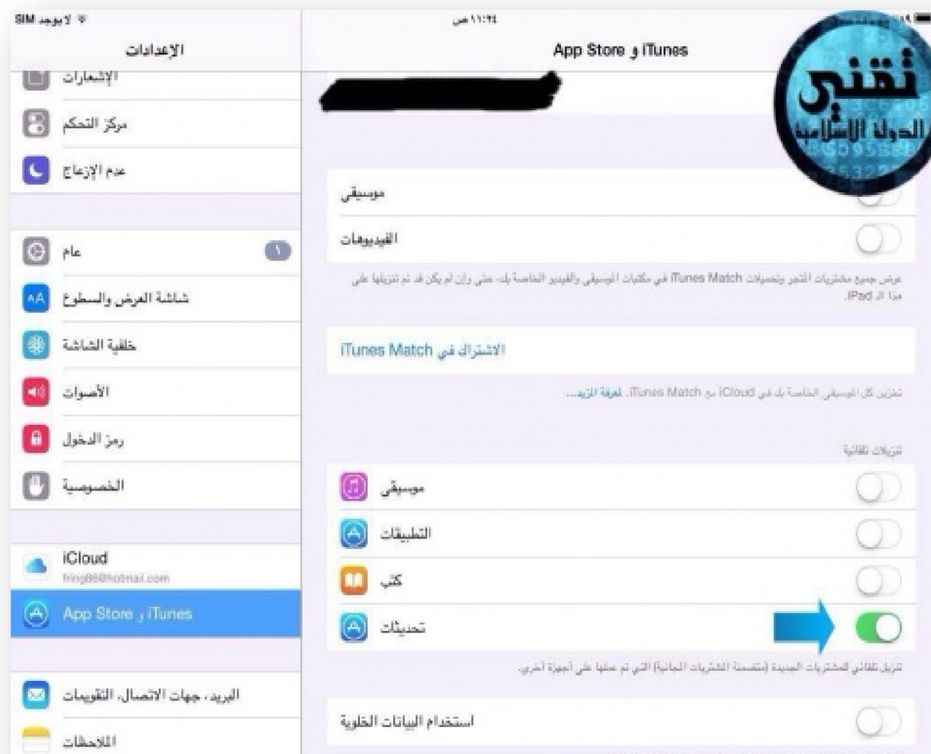
إن كنت متابع جيد للاخبار التقنية ستلاحظ ان كل اسبوع يكتشف باحثين أمنيين ثغرات جديدة في أنظمة التشغيل لذا فإن تحديث النظام بشكل مستمر أمر ضروري لتجنب الاختراق لكن قبل التحديث مباشرة يجب ان تنتظر قليلا لتتاكد ان النظام الجديد خالي من الاخطاء والثغرات

- التحديثات التلقائية للتطبيقات -

قم بتفعيل التحديث التلقائي للتطبيقات فالتحديث يساهم بحل مشاكل كثيرة ربما قد تكون سببا لاختراقك

تابع الخطوات

-



منع الوصول إلى الميكرفون الخاص بالهاتف -

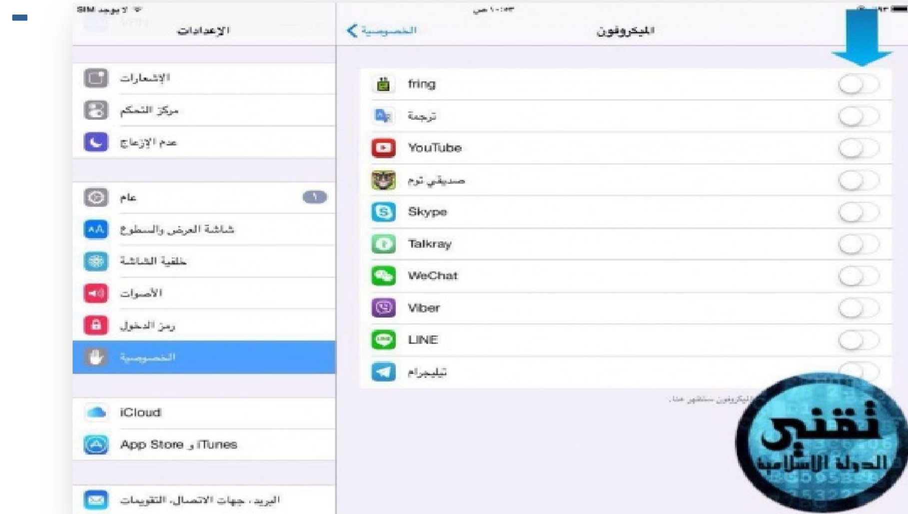
تابع الخطوات



ستظهر قائمة بالتطبيقات التي تستخدمه اغلقه امام كل تطبيق

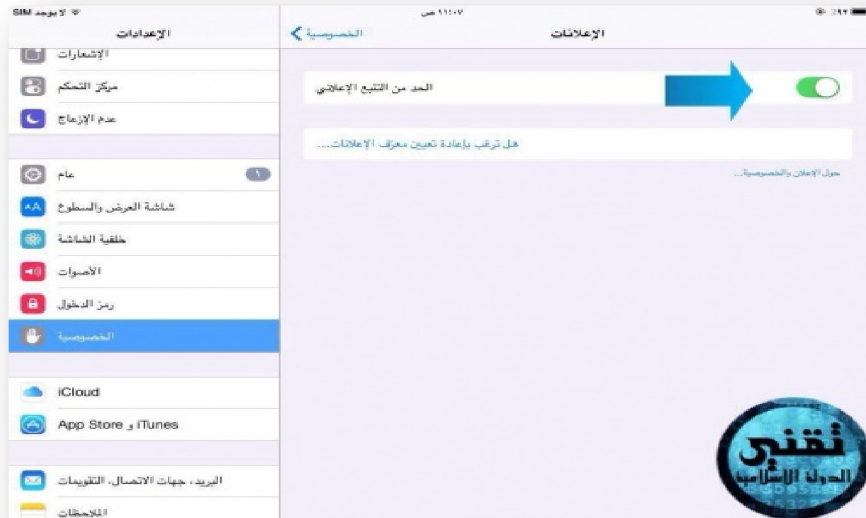
عدا التطبيقات المراد استخدامها صوتيا كالسكايب والفايبر

-



تفعيل الحد من التعقب الإعلاني -

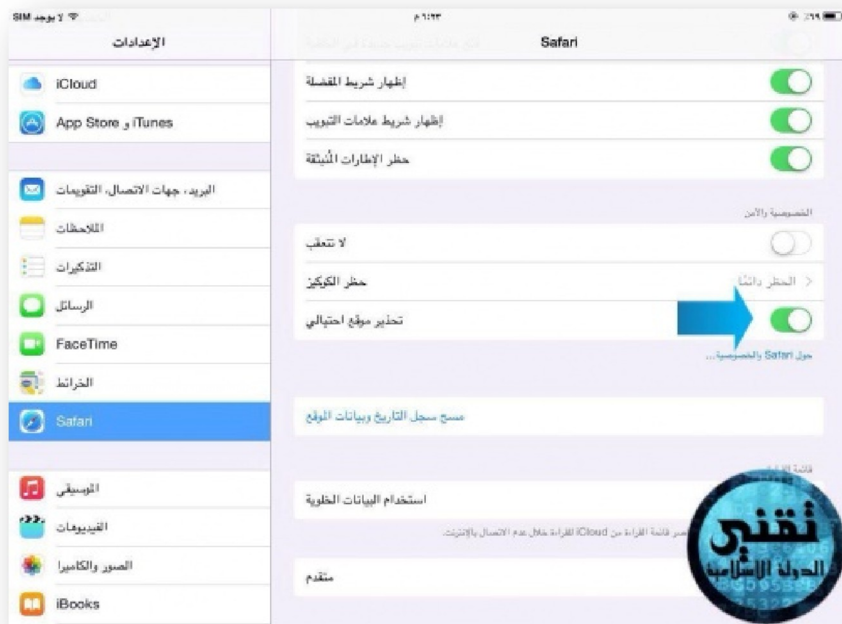
تابع الخطوات





- تفعيل تحذير موقع احتيالي -

وهى ميزة تسعى لمعرفة أن هذا الموقع محتال وتخبرك



- اي كلاود -

لا تقم بمزامنة الملفات لديك علي اي كلاود والافضل عدم تفعيله مطلقا

تابع الخطوات



تشفير أجهزة اللآيفون

من المميزات التي تتمتع بها أجهزة الآيفون هو وجود شريحة تشفير خاصة بكل جهاز "Encryption Chip" بحيث يتم فيها ومن خلالها حفظ شهادة التشفير ومفتاح التشفير الخاص بك، والذي من خلاله تستطيع تشفير كامل محتويات جهازك، وعند حذف أو تدمير هذا المفتاح فلن يستطع أحد الوصول للبيانات، وهذه الشهادة "مفتاح

التشفير" هي التي تجعل البيانات بجهازك قابلة للقراءة بعد إدخال الرقم السري.

الفرق في تشفير البيانات بين نظام آبل iOS7 و iOS8

كلا النظامين يدعم التشفير بشكل كبير وممتاز، وكان يسبب مشكلة كبيرة أمام جهات التحقيق حيث يصعب كسر تشفير هاذين النظامين خاصة إذا تم حمايتهم برقم سري قوي ومعقد وليس ٤ أرقام فقط.

إلا أن شركة آبل كانت تستطيع هي تجاوز الرقم السري الخاص بأي شخص عند حصولها على الجهاز، وكانت تساعد مكتب التحقيقات الفيدرالي الـFBI بشكل قانوني عند مصادرة أي جهاز، بحيث تتجاوز الرقم السري الخاص بالمتهمين وتحصل على البيانات التالية: -

١ - الإيميل الخاص بالمتهم وكل بريده الإلكتروني.

٢ - الصور ومقاطع الفيديو والتسجيلات الصوتية والرسائل القصيرة SMS وجهات الإتصال كلها.

٣ - كافة البيانات في البرامج والتطبيقات الخاصة بآبل مثل "النوتات، الرزنامة، الخرائط ومتصفح سفاري وهكذا.

لكن لم تكن شركة آبل قادرة على الدخول على التطبيقات الأخرى الغير خاصة بها، مثل تطبيق تويتر أو متصفح غير السفاري أو الواتساب او تيليجرام وغيره.

كما كانت توفر هذه الخدمة لمكتب التحقيقات الفيدرالي الـFBI بشكل كبير، ولكن أيضاً لبقية الدول ومنها العربية ولكن بشروط معقدة، ونادراً ما كان يأتيها حسب بعض تقارير الشفافية التي نشرتها.

ولكن .. ما سبق كله كان فقط في نظام iOS7 وما قبله، أما في نظام iOS8 الجديد، فكل ماسبق أصبح من الماضي ولا تستطيع الآن شركة آبل توفير مثل هذه المعلومات لجهات التحقيق مثل الــFBI ولا غيرها ممن يتقدم بمذكرات قانونية، وأصبح نظام التشفير الجديد يشفر كافة محتويات الجهاز وكل البرامج ومنها برامج آبل نفسها مثل الصور ومقاطع الفيديو والإيميل وغيرها، وهذه نقطة تحسب لشركة آبل.

كيفية تفعيل التشفير في جهاز الآيفون بنظام iOS8 ! وأفضل النصائح الأمنية الأخرى

سنشرح هنا أفضل طريقة للتشفير وحماية الجهاز، وليس أسهل طريقة:-

١- من جهاز الآيفون الخاص بك، إذهب الى الإعدادات "Settings" ثم الى قسم رمز الدخول "Passcode"

٢- قم بعد ذلك بتعطيل قسم "رمز دخول بسيط" – " Simple Password" وذلك لإستخدام كلمة مرور طويلة وليست فقط "٤" أرقام، وفي حالة إستخدامك لكلمة مرور وتكون فقط أرقام مثلا "١٠" أرقام، ستكون لوحة المفاتيح عند دخولك لجهازك فقط أرقام، ويفضل هنا إستخدام كلمة سر قوية، ولكن أكثر الناس لايرتاحون لذلك خاصة لحاجته دخول الجهاز مرات كثيرة، فيفضل مثلا إستخدام على الأقل "٦" أرقام، خاصة أن أجهزة آبل مصممة بطريقة دفاعية تقوم بعمل "تباطيء وتضع توقيت يأخر عملية إعادة ادخال الرقم السري" ضد من يعبث بجهازك، فسيعجز ويطول عليه الأمر، وهذه الطريقة الدفاعية أيضا مصممة للحماية من الأجهزة الخاصة بالتحقيق الجنائي، وهذه نقطة جيدة.

٣ - أدخل قسم "يتطلب رمز الدخول" – "Require Passcode" وإختار "حالاً" – Immediately ليتم قفل الجهاز فوراً عند إغلاق الشاشة.

٤ - بعد ذلك قم بتفعيل الـ Passcode وذلك بالضغط على تفعيل رمز الدخول "Turn Passcode On"

٥ - ثم سيطلب منك إدخال رمز الدخول ويفضل ألا يقل عن ٦ أرقام.

٦ - بعد إدخال "رمز المرور" الجديد ستظهر لك رسالة في آخر الصفحة وهي "تم تمكين حماية البيانات" – "Data Protection is enabled" كما في الصورة:

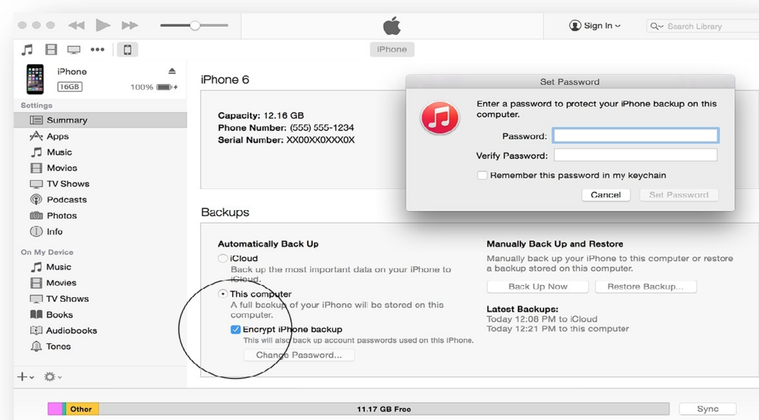


هنا تم تفعيل تشفير الجهاز بالكامل وكافة البيانات التي فيه.

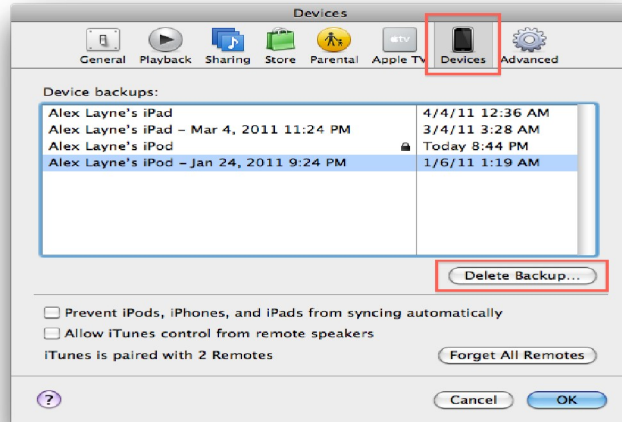
٧ - يفضل تفعيل خيار "مسح البيانات" – Erase Data – في حالة خوفك من مصادرة جهازك أو سرقته او في حالات السفر او المناسبات العامة التي قد يكثر فيها المتطفلون، وفي حالة تفعيلك لهذه الخاصية

فإن كافة بياناتك بالجهاز سيتم حذفها الى الأبد بعد "١٠" محاولات خاطئة لوضع رمز الدخول، ولن تتمكن من إسترجاعها.

٨- لاتقم بإستخدام النسخ الإحتياطي في الــ iTunes إلا في حالة تشفير النسخة الإحتياطية، ويتوفر ذلك في واجهه برنامج الــ iTunes وتأكد من وضع كلمة سرية قوية، أكثر جهات وبرامج التحقيق الجنائي تقوم بتحليل جهاز اللابتوب للبحث عن النسخ الإحتياطية لتحليلها، وإذا وجدتها مشفرة فتحاول كسر تشفيرها عن طريق وضع أرقام سرية عشوائية، إما إذا كانت النسخ الإحتياطية غير مشفرة، فقد كشفت نفسك تماماً في الصورة التالية يتبين لك كيفية تشفير النسخ الإحتياطية.



٩- في حالة عدم تأكدك من وجود نسخة إحتياطية بجهازك اللابتوب أو الدسكتوب يمكنك الدخول للإعدادت والتأكد من وجود نسخ أحتياطية سابقة أو لا، كما يبين لك حالتها من حيث التشفير من عدمه، وتستطيع حذف النسخ غير المشفرة كما في الصورة.



١٠- لا تخبر أحداً برقم جهازك السري أبداً، خاصة زوجتك وأطفالك .. فهم نقطة ضعف كبيرة عليك.

١١- لا تقم بإستخدام ولا إنشاء حساب iCloud لتحظى بأكبر قدر من الأمان والتشفير، وعند إستخدامك لخدمات iCloud فإن كل ما تشاركه في الخدمة يكون متاحاً لشركة آبل وتستطيع الوصول اليه عند طلب جهات التحقيق ذلك، لذلك يفضل عدم تفعيل الخدمة وعدم مشاركة بياناتك الخاصة مع شركة أبل حتى.

ولكن إن كان ولابد لك من إستخدام خدمات iCloud فإن كافة البيانات تنتقل لشركة آبل بشكل مشفر وآمن، كما تخزن في سيرفراتها بشكل مشفر، وهذا يحميك من الهاكرز أو الجواسيس وحتى من الحكومات التي تحاول إعتراض البيانات وتحليلها، ولكن لايحميك في حالة صدور مذكرة تفتيش امريكية.

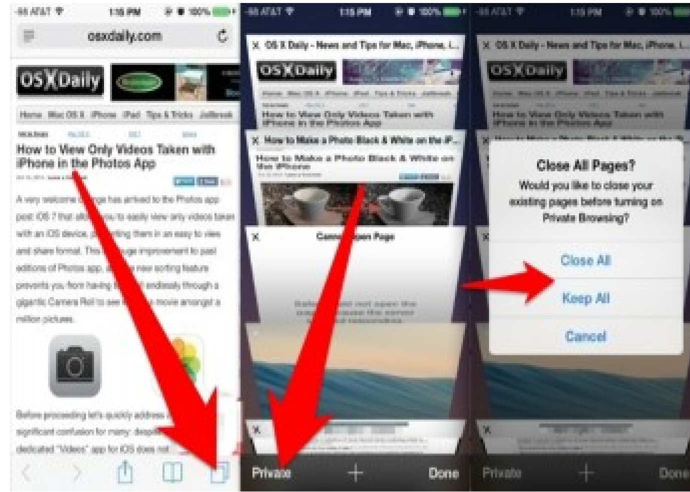
١٢- يكون تشفير آبل فعالاً بشكل كامل في حالة إغلاق الجهاز كلياً، أو إعادة تشغيله مع عدم فتح القفل بعد إعادة التشغيل، لذلك إذا أحسست بالخطر، فالأفضل هو إغلاق الجهاز أو اعادة تشغيله بسرعة مع عدم فتح القفل.

١٣- عند حاجتك لتفعيل خدمة مثل Find My iPhone لحماية بياناتك ومسح جهازك عند سرقته خاصة للناس كثيرو السفر والترحال، شخصياً أفضل عدم إستخدمها لأنها ستعطي لشركة آبل وصول لجهازك أيضاً، فإن كنت مضطراً لإستخدامها، فيفضل إستخدام خدمات مستقله عن آبل وتقدم نفس الخدمة مثل Anti-Theft Prey أو Lookout أو Security Mobile Security Avira الألمانية أو Anti Hidden Theft وغيرها، والمقصد هو أن بعثرة بياناتك بين الشركات أفضل من حصرها عند شركة واحدة مثل آبل.

١٤- وضع برامج تجسس في أجهزة الآيفون أمر ليس بالسهل، لذلك يحتاج الهاكر أو الجاسوس عمل "جيل بريك" – Jailbreak – لجهازك قبل ذلك، وهناك طرق يقوم بها الهاكر والجاسوس يستطيع من خلالها عمل "جيل بريك" بسرعة ثم يخفي أي آثار قد تجعلك تشك أن جهازك تم كسر حمايته، ثم بعد ذلك يزرع برنامج التجسس ويخفيه، لذلك يجب عليك التأكد من أن جهازك سليم ولم يتم عمل Jailbreak له، عن طريق تحديث الجهاز دائماً، أو إستعمال برامج مثل SnapStats الذي يخبرك بتفاصيل عن جهازك الآيفون منها هل هو Jailbroken أو لا!

١٥- يفضل تعطيل تخزين الكلمات السرية في متصفح سفاري وتعطيل ذلك من الإعدادات ثم السفاري ثم قسم الرقم السري " Password & AutoFill " وتعطيل كافة الخيارات فيه.

١٦- يفضل أستخدام خاصية "التصفح الخاص" في السفاري، بحيث لا يخزن أي معلومات عنك وعن الصفحات التي تزورها، وسيتحول المتصفح للون الأسود بعدها، ويكون بهذه الطريقة:



١٧ - هناك بعض البرامج التي تحتوي من نفسها أيضاً خاصية وضع رقم سري خاص للدخول عليها مثل تطبيق Threema يفضل أيضاً تفعيها لزيادة حماية البيانات الخاصة بالتطبيق.

١٨ - اذا كنت ممن يستخدم نظام "البصمة" في الآيفون والتي الى الآن تعتبر آمنة ولا تشاركها آبل مع نفسها ولا مع أي طرف ثالث، فيفضل إستخدام كلمة سر قوية من "أرقام وحروف" كرمز للدخول، لأنك تدخل بالبصمة فلن تحتاج الدخول بالرمز السري ولكن بقاء الرمز السري قوياً يبقيك آمناً عند محاولة أي شخص من الدخول على جهازك بطريقة غير شرعية، إلا إذا كنت تخشى أن يتم إجبارك على وضع إصبعك، وقام أحد بقطع يدك أو أصبعك للحصول على بصمتك! فابقى على رمز الدخول فقط وبدون استخدام "البصمة"

منقول

المصدر: https: / / blog.cyberkov.com / 2002.html

- كلمة المرور -

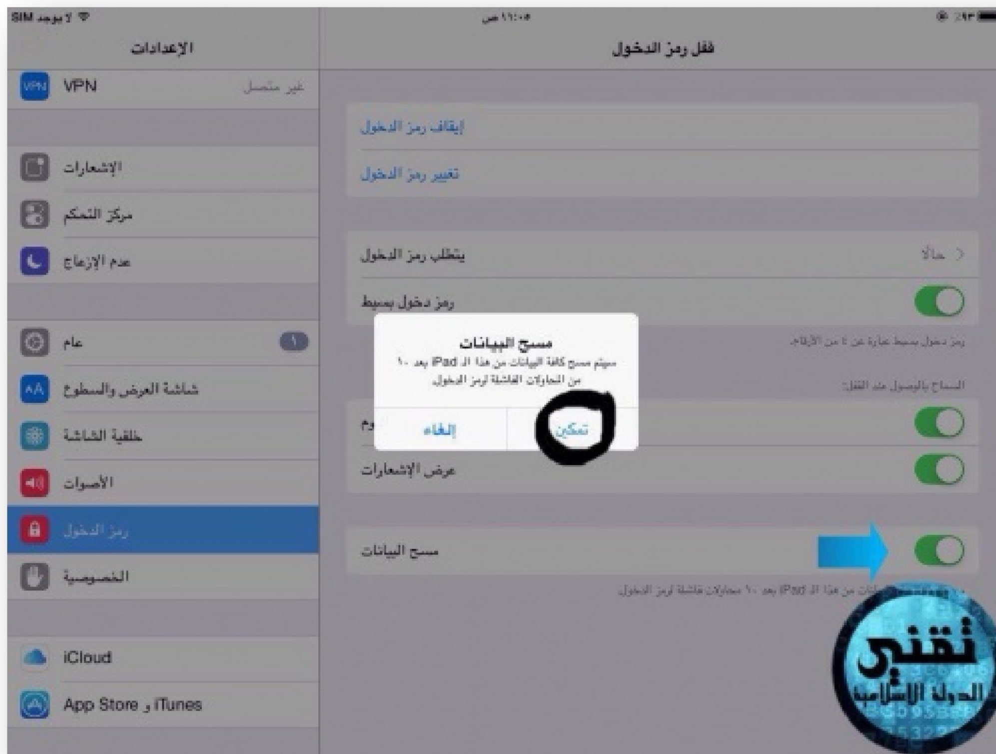
يجب ان تكون مكونة من ارقام وحروف صغيرة وكبيرة ورموز

ليصعب تخمينها بال

ATTACK DICTIONARY

وتفعيل خاصية مسح البيانات بعد ١٠ محاولات فاشلة لرمز الدخول

تابع الخطوات

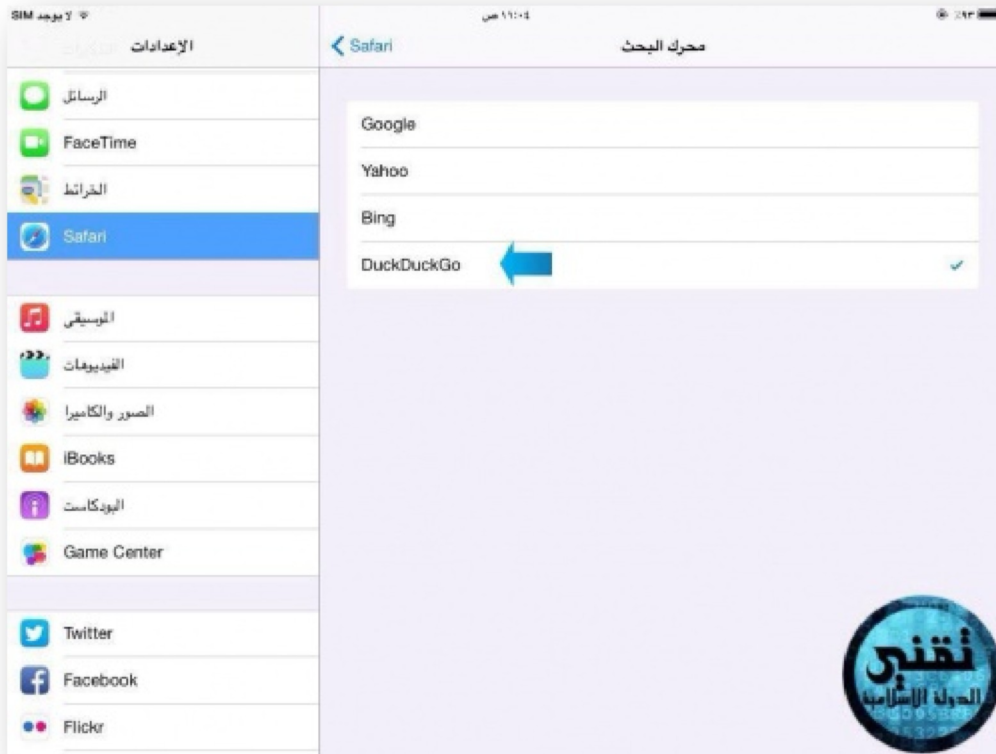


- متصفح سفاري -

قم باختيار المتصفح الافتراضي

GO Duck Duck

تابع الخطوات



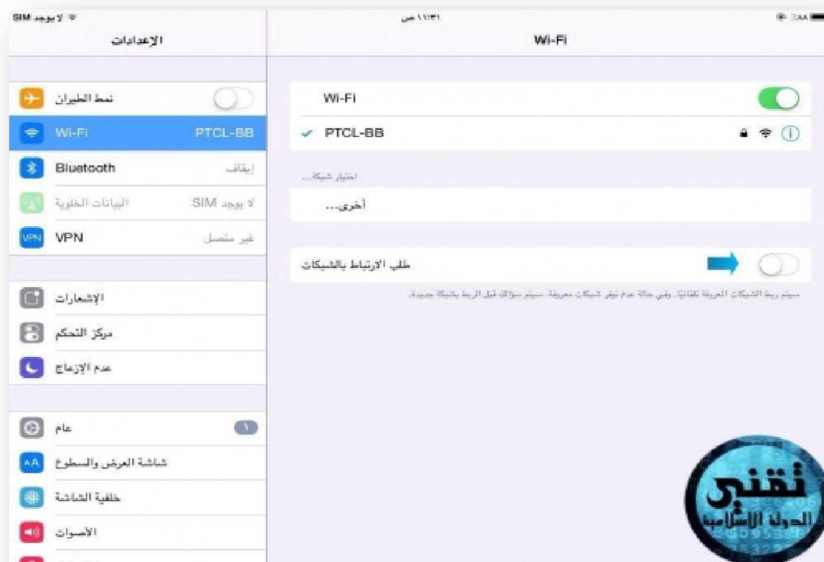
قم ايضا بمنع الكوكيز وتفعيل خاصية عدم التعقب في سفاري

تابع الخطوات



- الدخول التلقائي للشبكات -

قم بتعطيل خيار طلب الدخول التلقائي للشبكات فقد يتم توصيل جهازك الايفون دون علمك لاحد الشبكات ويتم اختراقك



- الموقع الجغرافي –

قم بتعطيل خيارالموقع الجغرافي لمنع تتبعك من قبل البرامج بجهازك



- برامج التصفح الامن -

استخدم برنامج

Onion browser

او

Broswer Open door / VPN

لاتنسونا من صالح دعائكم

- دروس أمنية:
- دورة أمن الهواتف الذكية
- دورة احتراف لينكس منت
- الحرب الالكترونية وغفلة انصار المجاهدين
- وداعــــا لجوجـــل ويــــاهو ومرحبــــا بالبريـــــد الالكتروني المشفر
- Smartphone security
- تايلز افضل وأأمن نظام تشغيل
- الأرشيف التقني





للدعم الفني تواصل معنا على

 | SR444TAW  | Tech_Support